



Defense Information Systems Agency

A Combat Support Agency

Test & Evaluation of the NR-KPP

Danielle Mackenzie Koester
Chief, Engineering and Policy Branch
July 14, 2010



Purpose



Provide an overview of the policies, processes and procedures for assessing compliance with the Net-Ready Key Performance Parameter





JS - Interoperability Certification

DOT&E - Operational Test Reports

DODD 4630.5

"IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life ..."

CJCSI 6212.01E

"All IT and NSS must be evaluated and certified for Joint interoperability by DISA (JITC)."

Title 10 United States Code (USC)

Section 2223

IT: Additional Responsibilities of DoD CIO
"Ensure the interoperability of Information Technology and National Security Systems throughout the DoD."

DODI 4630.8

"All IT and NSS ... must be tested for interoperability before fielding ... and certified by DISA (JITC)."

CJCSI 3170.01G

Establishes JCIDS w/ NR-KPP for CDD and CPD

DoD 5000 series

"For IT systems, including NSS, .. JITC shall provide system interoperability test certification memoranda ... throughout the system life-cycle and regardless of ACAT"

DODD 5105.19, "DISA"

Directs DISA to establish an OTA

DODD 5141.2, "DOT&E"

Lists the five recognized OTAs, including (JITC).

Title 10 United States Code (USC)

Section 139: "The Director [OT&E] shall prescribe... policies and procedures for the conduct of OT&E in the DoD...and report test results to Congress..."

Section 2399: OT&E must be adequate, and determine operational effectiveness and suitability

DODI 5010.41, JOINT TEST & EVALUATION (JT&E) PROGRAM

"A JT&E is OT&E that brings Military Departments together to assess Service interoperability in joint operations."

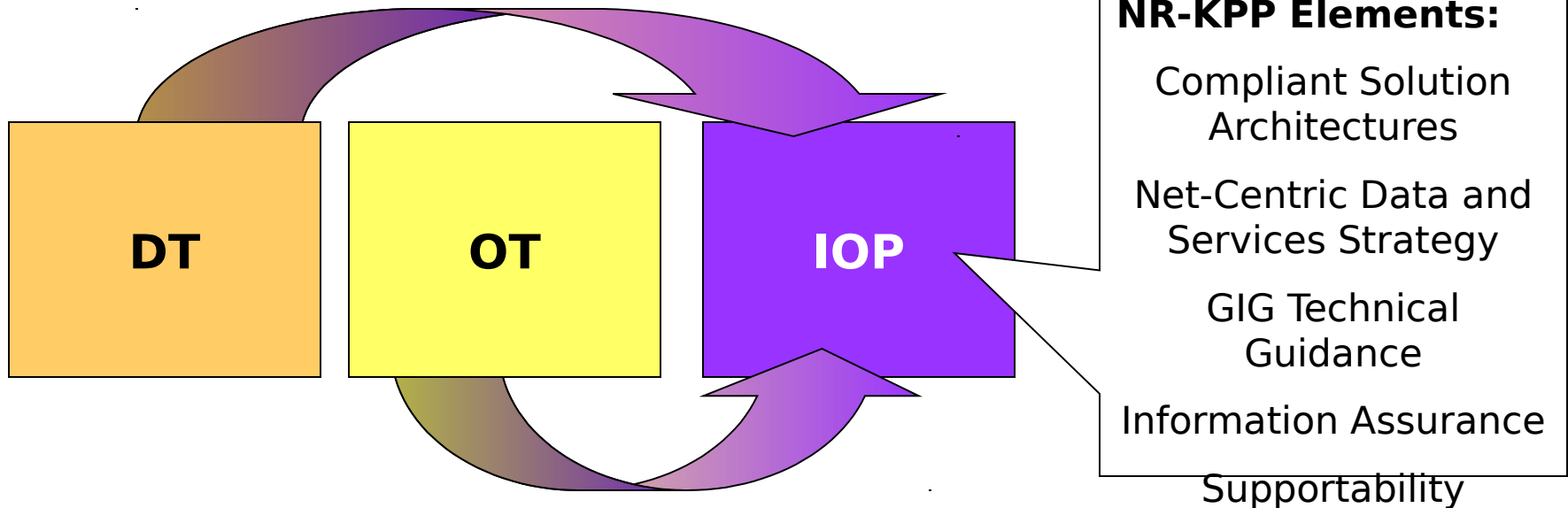
DISA INSTRUCTION 640-195-1 TEST & EVALUATION (T&E) OTA MISSION

"JITC shall perform the OTA mission... The Commander, JITC, will report directly to the Director, DISA, on OT&E matters."



DISA Joint Interoperability Test Certification Overview

A Combat Support Agency



- The NR-KPP elements define the areas JITC evaluates for interoperability certification
- JITC uses data collected during DT, OT, demonstrations, exercises, or other reliable sources for interoperability evaluations

Success = Minimizing separate interoperability testing by leveraging DT/OT

NR-KPP T&E Process

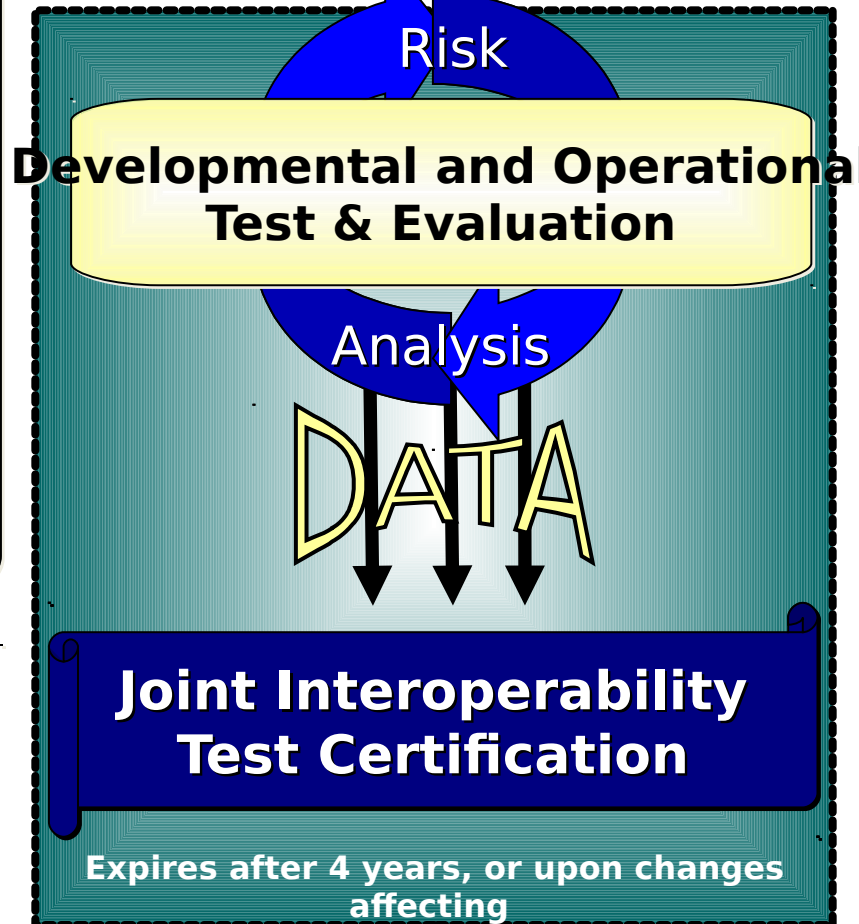


Joint Staff J-6

Interoperability & Supportability Certification Documents:

CDD, CPD, ISP, ISP Annex and TISP

JITC Test & Certification



NOTE:
Interoperability changes require reentering process at appropriate point:

- ✓ Requirements updates
- ✓ J-6 I&S Certification
- ✓ JITC Test & Certification



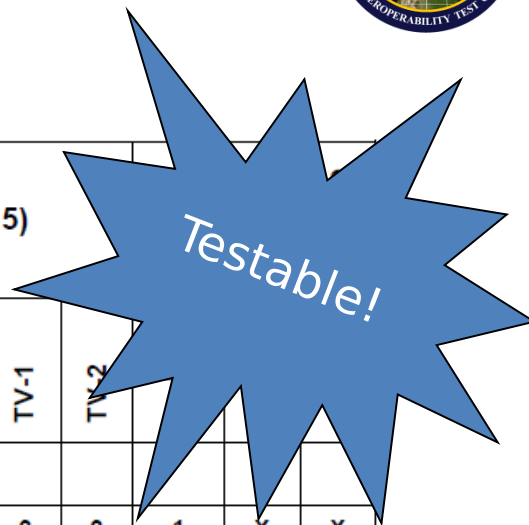
NR-KPP Statement



| KPP | Threshold | Objective |
|---|--|--|
| <p>Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.</p> | <p>The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include:</p> <ol style="list-style-type: none"> 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the | <p>The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include:</p> <ol style="list-style-type: none"> 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the |

Testable?

NR-KPP Requirements Source



| Document | Supportability Compliance | DOD Enterprise Architecture Products (IAW DODAF) (see Note 5) | | | | | | | | | | | | | | | | | | |
|------------------------|---|---|------|------|------|------|------|-------|------|------|------|------|------|------|-------|------|------|---|---|---|
| | | AV-1 /AV-2 | OV-1 | OV-2 | OV-3 | OV-4 | OV-5 | OV-6C | OV-7 | SV-1 | SV-2 | SV-4 | SV-5 | SV-6 | SV-11 | TV-1 | TV-2 | | | |
| ICD | | | X | | | | | | | | | | | | | | | | | |
| CDD | X | 3 | X | X | X | X | X | X | | | X | X | X | X | | 2 | 2 | 1 | X | X |
| CPD | X | 3 | X | X | X | X | X | X | 1 | | X | X | X | X | 1 | 2 | 2 | 1 | X | X |
| ISP | X | 3 | X | X | X | X | X | X | 4 | | X | X | X | X | 4 | 2 | 2 | 1 | X | X |
| TISP | X | 3 | X | | X | | X | X | | X | | | X | X | | 2 | 2 | 1 | X | X |
| ISP Annex (Svcs/ Apps) | X | 3 | X | | | | X | | | | X | X | X | X | | 2 | 2 | 1 | X | X |
| X | Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c) | | | | | | | | | | | | | | | | | | | |
| Note 1 | Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services, | | | | | | | | | | | | | | | | | | | |
| Note 2 | The TV-1 and TV-2 are built using the DISOnline and must be posted for compliance. | | | | | | | | | | | | | | | | | | | |
| Note 3 | The AV-1 must be uploaded onto DARS and must be registered in DARS for compliance | | | | | | | | | | | | | | | | | | | |
| Note 4 | Only required for Milestone C, if applicable (see Note 1) | | | | | | | | | | | | | | | | | | | |
| Note 5 | The naming of the architecture views is expected to change with the release of DODAF v2.0 (e.g., StdV, SvcV, StdV, DIV). The requirements of this matrix will not change. | | | | | | | | | | | | | | | | | | | |

Testable



Mapping NR-KPP to Operational Impact

(notional example)



| Capability | Operational Activity | System Function | Interface | Data & Services | Standards |
|------------|---------------------------------------|-------------------------------------|-----------------------------------|---|----------------------------|
| JMT | OV-5 | SV-4 | SV-6 | EVTS | TV-1 |
| Joint C2 | Understand Blue Force Resource States | Blue Force Location Auto Track Feed | (T) FBCB2 EPLRS (T) BFT SATCOM | Service: Blue Force Ground Data - Current | WSDL UDDI XML |
| | | Blue Force Location ISR Sensors | (T) BFT SATCOM (O) DCGS-A | Service: Blue Force Ground Data - Projected Data: JBFSA Schema/BFT | WS-I Basic Profile SOAP |
| | | | | | |

Compliant Solution Architectures
(Operationally Effective Information Exchanges)

Net-Centric Data & Services
GIG Technical Guidance

Information Assurance & Supportability





A Combat Support Agency

Operationally Effective Information Exchanges



NR-KPP Statement (Threshold)

...to include solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges"

CJCSI 6212.01E





A Combat Support Agency

Operationally Effective Information Exchanges



- **Requirements Analysis**

- **OV-5/6c (and other viewpoints as needed) are used to determine mission requirements, functions, and activities**
- **OV-3/SV-6 are used to determine interoperability criteria, e.g.**
 - **Timeliness**
 - **Accuracy**
 - **Completeness**

- **Test Planning and Execution**

- **Leverages all program lifecycle testing for data collection**
- **Interoperability testing of information exchanges must be on production representative system in an operationally realistic environment**
 - **Network**
 - **Loading conditions**





A Combat Support Agency

Operationally Effective Information Exchanges



Reporting

- **Threshold:** Meets all *joint critical* information exchange requirements contained in the J-6 certified NR-KPP
- **Objective:** Meets all information exchange requirements contained in the J-6 certified NR-KPP



DISA Data & Services Strategies

NR-KPP Statement (Threshold)

A Combat Support Agency



...to include compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications”

CJCSI 6212.01E



DISA Data & Services Strategies

Requirements Sources

A Combat Support Agency



Department of Defense
Net-Centric Data Strategy

Department of Defense
Net-Centric Services Strategy

Strategy for a Net-Centric, Service Oriented DoD Enterprise

Service Exposure Verification Tracking Sheet for <program>

Key: ☐ = In-Progress ☐ = Progress at Risk ☐ = Progress Stopped ☐ = Objective Achieved ☐ = Not Applicable

| Project POC Telephone # email address | Visible | Accessible | Understandable | # of Objectives Achieved Since Previous Submission |
|---|-----------------------------------|--|----------------------------------|---|
| IT System MTPR Number | MDR (1.a) | UDOI (1.b) | UDOI (2.a) Policy (2.b) | MDR (3.a) COI (3.b) |
| Submission Pkg Name | Service Description | (Note: Use above Key to assign values for columns below) | | |
| Issues/Comments | Exposure Start / Complete Date | | | |

Data Exposure Verification Tracking Sheet for <program>

Key: ☐ = Not Started ☐ = In-Progress ☐ = Progress at Risk ☐ = Progress Stopped ☐ = Objective Achieved ☐ = Not Applicable

| Program Manager Telephone # email address | Project POC Telephone # email address | Visible | Accessible | Understandable | # of Objectives Achieved Since Previous Submission | |
|---|---|----------------|--|----------------|---|-----------------|
| Web Page URL | IT System DITPR Number | CD&D (1.a) | Policy (2.a) | Oper (2.b) | User (3.a) | |
| Top Level JCA | Data Asset | Description | (Note: Use above 'Key' to assign values for columns below) | | | Submission Date |
| (JCA Category) | Asset #1 | Description #1 | | | | |
| | Asset #2 | Description #2 | | | | |
| | Asset #n | Description #n | | | | |
| (JCA Category) | Asset #1 | Description #1 | | | | |
| | Asset #2 | Description #2 | | | | |
| | Asset #n | Description #n | | | | |
| (JCA Category) | Asset #1 | Description #1 | | | | |
| | Asset #2 | Description #2 | | | | |
| | Asset #n | Description #n | | | | |

<CLASSIFICATION>

Version 0.1, 7 DEC 07

Department of Defense
Information Enterprise Architecture Version 1.1



May 2009

Prepared by:
Department of Defense
Office of the Chief Information Officer

DISA Data & Services Strategies

A Combat Support Agency



Data Strategy Compliance

Visible

Accessible

Data Management

Understandable

Trusted

Interoperable

Responsive to User's Needs

Services Strategy Compliance

Provide Services

Use Services

Govern the Infrastructure and Services

Monitor and Manage Services via GIG NetOPS

DoD Information Enterprise Architecture Compliance

Data and Services Deployment

Secured Availability

Shared Infrastructure Environment

Computing Infrastructure Readiness

NetOPS Agility



Data Strategy Compliance

Visible

Accessible

Data Management

Understandable

Trusted

Interoperable

Responsive to User's Needs

"Discovery Metadata shall conform to DDMS"

"Post descriptions of access mechanisms"

"Associate data pedigree metadata"

Services Strategy Compliance

Provide Services

Use Services

Govern the Infrastructure and Services

Monitor and Manage Services via GIG NetOPS

"Use DoD CIO mandated Core Enterprise Services"

"Define and advertise Service Level Agreements"



DISA Data & Services Strategies Requirements

A Combat Support Agency



Net-Centric Data Requirement

Data is Visible

Post discovery metadata in an Enterprise Catalog: Department of Defense (DoD) Discovery Metadata Specification (DDMS)- conformant discovery metadata is posted in the Net-Centric Enterprise Services (NCES) Enterprise Catalog or other compatible/federated enterprise catalog that is visible to the Enterprise.

Use appropriate keywords for discovery: Discovery keywords should reflect common user terms, be appropriate for mission area or data type, be understandable, and conform with MDR requirements that map back to COI identified mission data.

Data is Accessible

Post data to shared space: Data asset is available in a shared space, i.e., a space that is accessible to multiple end users.

Provide access policy: If data is not accessible to all users, a written policy on how to gain access is available and accurate.

Provide serving (access) mechanism: Shared space provides serving (access) mechanisms for the data. I.e., a service provides users with access to the data.

Publish active link to data asset: The Enterprise Catalog DoD Discovery Metadata Specification (DDMS) entry contains an active link (e.g., Uniform Resource Identifier (URI)) to the data asset.

Data is Understandable

Publish semantic and structural metadata

- Semantic and structural metadata are published in the Enterprise Catalog.

Register data artifacts in DoD MDR

- XML schema definitions (XSD), eXtensible Markup Language (XML) instances, data models (such as entity relationship diagrams) and other appropriate artifacts are registered in the DoD Metadata Registry (MDR).

Data is Interoperable

Base vocabularies on Universal Core (UCore)

- Semantic vocabularies reuse elements of the Universal Core (Ucore) standard.

Comply with COI data-sharing agreements

- Semantic and structural metadata conform to interoperability agreements promoted through communities, e.g., Community of Interest (COI).

Conform to DDMS

- All metadata, including record-level database tagging and in-line document tagging, complies with DDMS.

Data is Trusted

Provide information assurance and security metadata

- All metadata, including record-level database tagging and in-line document tagging, includes data pedigree and security metadata, as well as an authoritative source for the data (when appropriate).

Net-Centric Services Requirement

Services are Visible

Publish a description of the service or access mechanism

- Descriptions (metadata) for the service or access mechanism are published in an enterprise service registry, e.g., the NCES Service Registry.

Comply with enterprise-specified minimum service discovery requirements

- The data access mechanism complies with enterprise-specified minimum service discovery requirements, e.g., a Universal Description, Discovery and Integration (UDDI) description to enable federated discovery.

Services are Accessible

Provide an active link to the service in the enterprise catalog

- Active link (e.g., Uniform Resource Identifier (URI)) to the specified service is included in the enterprise catalog metadata entry (i.e., metacard) for the specified service.

Provide an active link to the service in the NCES Service Registry

- URIs as the operational end points for services shall be registered in the NCES Service Registry by referencing the WSDL (that is in the MDR).

Services are Understandable

Publish a description of the service or access mechanism to the NCES Service Registry

- Metadata for the service or access mechanism are published in the NCES Service Registry.

Publish service artifacts to DoD MDR

- Web Service Description Language (WSDL) documents, and other appropriate artifacts are registered in the DoD Metadata Registry (MDR).

Provide service specification or Service Level Agreement (SLA)

- A service specification or Service Level Agreement (SLA) exists for services and data access mechanisms.

Services are Trusted

Operate services in accordance with SLA

- The service meets the performance standards in the SLA

Include security mechanisms or restrictions in the service specification

- The service specification describes security mechanisms or restrictions that apply to the service

Enable continuity of operations and disaster recovery for services

- The service has a defined and functional Continuity of Operations Plan

Provide NetOps Data (NetOps Agility)

- Services and data access mechanisms provide operational states, performance, availability, and security data/information to NetOps management services, e.g., Enterprise Management, Content Management, and Network Defense services

Use of Core Enterprise Services (CES)

- Core Enterprise Services (CES) are used in accordance with DoD CIO mandates



DISA Data & Services Strategies

A Combat Support Agency



Does it apply?

| | |
|---|---|
| 1. Is the system only a transmission device such as a radio, satellite, or network equipment? Transmission Devices are communications devices which provide connectivity, but do not handle data except in encapsulated form. | |
| YES: THIS SYSTEM IS ONLY A TRANSMISSION DEVICE THE N-C DSS ELEMENT DOES NOT APPLY TO YOUR PROGRAM | NO: THIS SYSTEM IS NOT ONLY A TRANSMISSION DEVICE GO TO QUESTION #2 |
| 2. Does the system employ the use of Internet Protocol (IP) as a means of communication? IP is a protocol used for communicating data across a packet-switched internetwork. | |
| YES: THIS SYSTEM USES THE INTERNET PROTOCOL GO TO QUESTION #3 | NO: THIS SYSTEM DOES NOT USE THE INTERNET PROTOCOL THE N-C DSS ELEMENT DOES NOT APPLY TO YOUR PROGRAM |
| 3. Does the system employ only pre-defined "Point to Point" Information Exchanges? Point to Point information exchanges are pre-defined, engineered information exchanges that do not have provisions for unanticipated GIG users in their implementation. | |
| YES: THIS SYSTEM USES ONLY POINT TO POINT INFORMATION EXCHANGES THE N-C DSS ELEMENT DOES NOT APPLY TO YOUR PROGRAM | NO: THIS SYSTEM DOES NOT USE ONLY POINT TO POINT INFORMATION EXCHANGES GO TO QUESTION #4 |
| 4. Does the system have infrastructure or timeliness constraints that preclude implementation of the Net-Centric Data or Services Strategies? Do any of the following apply: <ul style="list-style-type: none"> System has network connectivity less than 85% of the time System resides on a network infrastructure with less than 100 kbps bandwidth Latency constraints are equal to or less than 1 second | |
| YES: THIS SYSTEM HAS ARCHITECTURE CONSTRAINTS PRECLUDING IMPLEMENTATION THE N-C DSS ELEMENT DOES NOT APPLY TO YOUR PROGRAM | NO: THIS SYSTEM DOES NOT HAVE ARCHITECTURE CONSTRAINTS PRECLUDING IMPLEMENTATION GO TO QUESTION #5 |
| 5. Does the system consume or provide Enterprise-Level Net-Centric Data or Services? Enterprise-level net-centric data is designed for use across Command, Component, Service or Agency boundaries and is to be used by both anticipated and unanticipated users. Enterprise-level net-centric services are designed for use across Command, Component, Service or Agency boundaries and are developed in the form of loosely-coupled software services, using any service-based technology. | |
| YES: THIS SYSTEM CONSUMES OR PROVIDES ENTERPRISE-LEVEL NET-CENTRIC DATA OR SERVICES THE N-C DSS ELEMENT DOES APPLY TO YOUR PROGRAM | NO: THIS SYSTEM DOES NOT CONSUME OR PROVIDE ENTERPRISE-LEVEL NET-CENTRIC DATA OR SERVICES THE N-C DSS ELEMENT DOES NOT APPLY TO YOUR PROGRAM |





- **Requirements Analysis**
 - Determine applicability of net-centric requirements
 - Determine enterprise-level shared data and services as defined in JS-certified requirements documents: Exposure Verification Tracking Sheet (EVTS) (“Blue Sheets”)
- **Risk Assessment - Joint Critical vs. Contributory**
- **Test Planning and Execution**
 - Conduct initial static analysis (e.g., registration of assets)
 - Execute conformance/compliance testing (e.g.,





- **Threshold:** Meets all *joint critical* net-centric requirements contained in the J-6 certified NR-KPP
- **Objective:** Meets all *net-centric* requirements contained in the J-6 certified NR-KPP



...compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views”

CJCSI 6212.01E



DISA GIG Technical Guidance

Requirements Sources

A Combat Support Agency



DISRonline DoD Information Technology Standards Registry
UNCLASSIFIED

FAQs
DISR Calendar
Reports & Archives

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER
You are accessing a U.S. Government (USG) Information System (IS) that is provided for authorized users only. By using this IS (which includes any device attached to this IS), you consent to the following:

- The USG routinely intercepts and monitors communications on this IS for purposes including network operations and defense, personnel misconduct (PM), law enforcement, and intelligence gathering.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls).
- Notwithstanding the above, using this IS does not constitute consent to PM, law enforcement, or intelligence gathering, or work product, related to personal representation or service.

Welcome to GTD Online
GESP Title: X-band Communication Waveforms
Reference ID: GESP-0002.0005
DIEA Area: Communications
GESP Version Number: 1.0
Version Date: 30 Sep 2008
[Return](#)

Interoperability Reference Architecture and Service Description
Infrastructure
Structure in the GIG consist of Fixed Infrastructure, Satellite Communications, and Tactical Edge Infrastructure as shown in Figure 1.

Fixed Infrastructure

- Network Ops
- Satellite Ops

Satellite Communications

- Narrowband
- Wideband
- Protected

Tactical Edge Infrastructure

- Non-IP
- IP-Based

Key Interfaces connect the three main categories.

GTG Sample Program
Program Questionnaire GESPs Declaration
Update Program
This screen gives you the opportunity to create a program. Please note, "*" indicates a required field.
*Program Name: GTG Sample Program
Acronym: GSP
DITPR ID: 56544323
Declaration Lock: ☐ declaration is locked for editing
*Start Date: 03 Nov 2008
*Organization: DISA
*POC: Donnelly, Josh Mr. ☐ POC not in system
Compliance Response Created By: Administrator, System
*GTG Version: GTG v1.0
Program Description: This is a sample program
[Save & Close](#) [Reset](#) [Close](#)

DISRonline Software
Software updated 2008

Internet
100%
10:04 AM Wednesday





- **Requirements Analysis**
 - Execute risk analysis on standards identified in system TV-1 using JITC Risk Assessment Database (J-RAD)
 - Determine standards that will be tested and appropriate test environments/methodologies
- **Test Planning and Execution**
 - Leverage commercial and government test results, as appropriate

frm_TV1_Builder : Form

Manage List of Standards or TV-1s

Close Save

Add New List/TV-1 View All Lists/TV-1s JITC Risk Report for this List/TV-1

Or Select a TV-1: CFMS TV-1 (Group: CFMS ; CSS: System)

Description:

In addition to standards shown for this list of standards or TV-1, you can also get standards from the following.

From Another List/TV-1: Get It!

From an Interest Group: Get It!

Get Emerging and Mandated DISR Standards in this Database! Get All Standards in this Database!

Only CHECKED items will be saved on your list of standards or TV-1. Unchecked items will be removed from your list but can be reselected.

| ANSI T1.102-1993 (R2005) | Digital Hierarchy - Electrical Interfaces, December 1993 |
|---|---|
| <input checked="" type="checkbox"/> CIM HTTP | Specification for CIM Operations over HTTP Version 1.0, Distributed Management Task Force, Inc., 11 August 1999 |
| <input checked="" type="checkbox"/> CIM XML | Specification for the Representation of CIM in XML Version 2.0, Distributed Management Task Force, Inc., 20 July 1999 |
| <input checked="" type="checkbox"/> CICS ISM: XML | Common Information Sharing Standard for Information Security Marking: XML Implementation, Implementation Guide, Release 2.0.3, 15 February 2000 |
| <input checked="" type="checkbox"/> Core Architecture Data Model (CADM) Baseline 1.03, 9 May 2006 | |
| <input checked="" type="checkbox"/> Core Architecture Data Model (CADM) Baseline 1.03, 9 May 2006 | |
| <input checked="" type="checkbox"/> FIPS Pub 10-4:2002 | Countries, Dependencies, Areas of Special sovereignty, and their Principle Administrative Divisions, April 1995 as modified by various Change Notices |
| <input checked="" type="checkbox"/> FIPS Pub 184 | Information Definition File Transformation Module (IDTF) - December 1993 |
| <input checked="" type="checkbox"/> GIG | SGSDB Version: 01.01.01 |

STANDARDS

Version: 01.01.01, 03/06/2009 20:20 MST
Currently linked to backend database: D:\BACKUP\IDBS\U_SGSDB_be_Test.mdb
Welcome Sivey Anderson

ADD/EDIT

Standards NCGIS Spotlight Form

Test Methodologies List of Standards or TV-1

Products / Test Tools

Producers

Interest Groups

Testing Organizations

Locations

Sources

Open Links to Sources

Contacts

Edit My Profile

QUERIES

Standards Table of Contents

Standards with JITC Risk Rationale

Database Information: Sivey Anderson, 520-538-0786, Sivey.Anderson.cri@disa.mil

Open the User's Manual

Note: GIG Enterprise Service Profiles are not yet mandated.





- **Threshold: No critical standards conformance-based deficiencies were identified in DT and OT by a combination of government and/or commercial verifications or JITC standards testing or conformance certifications that included all high-risk standards in the TV-1 that support a critical information exchange.**
- **Objective: No critical standards conformance-based deficiencies were identified in DT and OT by a combination of government and/or commercial verifications or JITC conformance certification for any high-risk standards in the TV-1.**





...to include Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA)”

CJCSI 6212.01E



DISA Information Assurance Requirements Sources

A Combat Support Agency



Department of Defense INSTRUCTION

NUMBER 8510.01
November 28, 2007

ASD(NII)/DoD CIO

SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)

- References:
- (a) Subchapter III of Chapter 35 of title 44, United States Code, "Federal Information Security Management Act (FISMA) of 2002"
 - (b) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
 - (c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
 - (d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
 - (e) through (ab), see Enclosure 1

1. PURPOSE

This Instruction:

- 1.1. Implements References (a), (b), (c), and (d) by establishing the DIACAP for authorizing the operation of DoD Information Systems (ISs).
- 1.2. Cancels DoD Instruction (DoDI) 5200.40; DoD 8510.1-M; and ASD(NII)/DoD CIO memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance" (References (e), (f), and (g)).
- 1.3. Establishes or continues the following positions, panels, and working groups to implement the DIACAP: the Senior Information Assurance Officer (SIAO), the Principal Accrediting Authority (PAA), the Defense Information Systems Network (DISN) Global Information Grid (GIG) Flag Panel, the IA Senior Leadership (IASL), the Defense (previously DISN) IA Security Accreditation Working Group (DSAWG), and the DIACAP Technical Advisory Group (TAG).
- 1.4. Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.



Department of Defense DIRECTIVE

NUMBER 8500.01E
October 24, 2002
Certified Current as of April 23, 2007

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA)

- References:
- (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
 - (b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
 - (c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
 - (d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
 - (e) through (ah), see enclosure 1

1. PURPOSE

This Directive:

- 1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
- 1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d), and (e)).
- 1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.
- 1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).





- **Requirements Analysis***
 - **Evaluate the status of the Certification and Accreditation (C&A) process (DIACAP, NISCAP, ICD 503)**
 - **All systems are required to receive an IATO/ATO (threshold) or ATO (objective) by the Designated Accrediting Authority (DAA)**
 - **All systems are required to complete interoperability and operational testing in the approved IA configuration as specified in the C&A package**
- **Test Planning and Execution**
 - **Ensure the system is operating in the approved IA configuration for interoperability and operational testing**
 - **Verify IATO/ATO**
 - **Execute required additional IA testing**

** Not all systems are required to comply with DoDI 8510.01*





- **Threshold: The Designated Accrediting Authority (DAA) has issued an Interim Authorization to Operate (IATO) or an Authorization to Operate (ATO) for the system**
- **Objective: The DAA has issued an ATO for the system**



Supportability

NR-KPP Statement (Threshold)



***...Supportability requirements to include
SAASM, Spectrum and JTRS requirements”***

CJCSI 6212.01E

Supportability Requirements Source



Department of Defense INSTRUCTION

NUMBER 4650.01
January 9, 2009

ASD(NII)

SUBJECT: Policy and Procedures for Management and Use of the Electromagnetic Spectrum

References: See Enclosure 1

1. **PURPOSE.** This Instruction:

a. Reissues DoD Directive (DoDD) 4650.1 (Reference (a)) as a DoD Instruction in accordance with the guidance in DoD Instruction (DoDI) 5025.01 (Reference (b)) and the authority in DoDD 5144.1 (Reference (c)).

b. Establishes policy, assigns responsibilities, and provides instructions for management and use of the electromagnetic spectrum in accordance with Reference (c).

c. Implements section 305 and chapter 8 of title 47, United States Code (Reference (d)); Office of Management and Budget (OMB) Circular A-11, Part 2, Sec. 33.4 (Reference (e)); and the Manual of Regulations and Procedures for Radio Frequency Management (Reference (f)).

2. **APPLICABILITY.** This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. **DEFINITIONS.** See Glossary.

4. **POLICY.** It is DoD policy that:

a. The electromagnetic spectrum (hereafter referred to as "spectrum") is a critical resource, and access to the spectrum is vital to the support of military operations. Proper management and use of the spectrum available to the Department of Defense shall be an integral part of military



Department of Defense

DIRECTIVE

NUMBER 3222.3
September 8, 2004

ASD(NII)

CT: DoD Electromagnetic Environmental Effects (E3) Program

- References: (a) DoD Directive 3222.3, "Department of Defense Electromagnetic Compatibility Program," August 20, 1990 (hereby canceled)
(b) JCS Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," September 28, 2002
(c) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004
(d) DoD 4120.24-M, "Defense Standardization Program Policies and Procedures," March 9, 2000

ISSUANCE AND PURPOSE

Directive:

1. Reissues reference (a) to update policy and responsibilities for the management and implementation of the DoD Electromagnetic Environmental Effects (E3) Program to ensure mutual electromagnetic compatibility (EMC) and effective E3 control among air, sea, and space-based electronic and electrical systems, subsystems, and equipment, and with the existing natural and man-made electromagnetic environment

2. Assigns responsibilities for the execution of the DoD E3 Program.

3. Promotes the following DoD E3 Program objectives:

1.3.1. Achieving operational EMC for all electronic and electrical systems, equipment, and equipment developed, acquired, and operated by the DoD Components. Mutual EMC and effective E3 control is achieved when systems, subsystems, and equipment operate in their intended EME without suffering unacceptable performance degradation from E3 or causing unintentional performance degradation to other systems.

CJCSI 6130.01D
13 April 2007

2007 CJCS MASTER POSITIONING, NAVIGATION, AND TIMING PLAN (MPNTP)



JOINT STAFF
WASHINGTON, D.C. 20318

This document contains information exempt from
mandatory disclosure under the FOIA.
Exemptions 2, 3 and 5 apply.

Supportability

Evaluation Procedures



- **Spectrum Supportability**
 - **Verify the system has an approved (Stage 4) DD Form 1494 (for any spectrum dependent system) (DoDI 5000.02)**
 - **Verify completion of applicable requirements of DODD 3222.2, "DOD Electromagnetic Environmental Effects (E3)"**
- **Selective Availability Anti-Spoofing Module (SAASM)**
 - **Verify any GPS receivers procured are SAASM or MGUE compliant (CJCSI 6130.01D)**
- **Joint Tactical Radio System (JTRS)**
 - **Verify a JTRS solution or waiver for any radio solution operating within the 2MHz to 2 GHz range***

**Reference: (ASD(NII)/DOD CIO memorandum, 23 May 2005, "Temporary Suspension of the Joint Tactical Radio Systems (JTRS) Waiver Process" and ASD(NII)/DOD CIO memorandum, 12 January 2007 "Reinstatement of the Joint Tactical Radio, (JTRS) Waiver Process for Handheld Radio Procurements")*



Supportability Reporting



- **Threshold = Objective:**
 - **Spectrum Supportability**
 - **Approved Stage 4 DD Form 1494**
 - **Verified E3 compliance**
 - **SAASM Compliance: If the system implements GPS, the receiver must be SAASM compliant or the program has a waiver from ASD(NII)**
 - **JTRS Compliance: If the system has a requirement for radio-based communications in the 2 MHz to 2 GHz range, the system must implement a JTRS solution or have authorization from ASD(NII)/DoD CIO for the specific procurement**





A Combat Support Agency

Interoperability Certification Products



| Certification | Description | System can be fielded (Y/N)? |
|---|---|------------------------------|
| Standards Conformance Certification | System is certified for conformance to a standard/standards profile | No |
| Joint Interoperability Test Certification | Full system certification. System meets at least <u>all critical</u> interoperability requirements | Yes |
| Limited Joint Interoperability Test Certification | System meets <u>subset</u> of critical interoperability requirements | Yes, with ICTO |
| Interim Joint Interoperability Test Certification | A capability module has adequately demonstrated interoperability for at least <u>all critical</u> threshold requirements identified for the increment | Yes |
| Special Interoperability Test Certification | Certification is based on other J-6 approved requirements other than the NR-KPP, e.g., use of UCR for voice switches | Yes |
| Non-Certification | Critical operational impacts expected Provides a warning to the warfighter | No |
| | PM would like to determine | |



DISA References & Resources

A Combat Support Agency



- **NR-KPP Helpdesk:** NR-KPP_Helpdesk@disa.mil
- **URLs for (Interoperability and Supportability) Internet resources are located on the CJSCI 6212 Resource Page:**
https://www.intelink.gov/wiki/Portal:CJSCI_6212_Resource_Page
- **JITC NR-KPP Guidebook:**
<https://www.intelink.gov/sites/jitc/nrkpp/guidebook/Wiki%20Pages/Home.aspx>
- **GIG Technical Guidance Federation:**
<https://216.181.4.90/gtg/login.do;jsessionid=18B78A357186110C75589197B31276A3?jsessionid=1268330917971&redirectUrl=>
- **JITC Data & Services 101 Tutorial:**
<https://connect.dco.dod.mil/p51771709/?session=breezuffahb84y7v7qz7v>
- **DISR Online Account Request:**
<https://disronline.disa.mil/a/public/consent>
- **DoD Metadata Registry:**
<https://metadata.dod.mil/mdr/homepage.htm>
- **JITC NR-KPP Helpdesk Wiki:**
https://www.intelink.gov/wiki/NR-KPP_Helpdesk



- **Hotline**
 - 24/7 C4I Technical Support
 - 1-800-538-JITC (5482)
 - hotline@disa.mil
 - <http://jitc.fhu.disa.mil/support.html>
- **Joint Interoperability Tool (JIT)**
 - <http://jit.fhu.disa.mil>
 - Lessons Learned reports
 - NATO Interface Guide
- **System Tracking Program (STP)**
 - <https://stp.fhu.disa.mil>
 - Test events
 - Test plans and reports
 - Certification results



General Testing Support

(301) 744-2681 or <http://jitc.fhu.disa.mil/gtsform.html>



Questions?

Danielle Mackenzie Koester
Danielle.Koester@DISA.mil
Chief, Engineering & Policy Branch
Joint Interoperability Test Command
July 14, 2010



